ABSTRACT
METHOD OF DETECTING ILLICIT MODIFICATIONS OF MANUFACTURER SOFTWARE

Method making it possible to detect and/or to avoid illicit modifications of manufacturer software within a GSM type system, comprising a hard kernel and a soft kernel, a local data interface, comprising at least the following steps:

A – the signal received on the local data interface of the terminal is not valid, place the GSM terminal in a disabled state,

B – the signal is a disconnection signal on the local data interface, or there is no signal, instigate a secure startup procedure, with execution of the control functions:

Auto test of the hard kernel

- If the auto test is OK, then test the integrity of the soft kernel
    - If this integrity is OK, then activate the terminal for normal operation,
    - If the integrity is KO, then place the terminal in a disabled state,
- If the auto test is KO, then place the GSM terminal in a disabled state.

C – the received signal is a valid startup signal:

- If the fuse is not blown, render the GSM terminal enabled,
- If the fuse is blown, render the terminal not totally enabled, by deactivating at least one of the enabled functions of the terminal:
    - If the signal is a signal of JTAG test type, continue the test procedure,
    - If the signal is a test signal, start up in nonsecure mode and continue the test procedure.

Figure 3 to be published